

# **C2W: A BATTLEFIELD OPERATING SYSTEM FOR FORCE XXI?**

**A MONOGRAPH  
BY  
Major Stephen M. Woolwine  
Military Intelligence**



**School of Advanced Military Studies  
United States Army Command and General Staff  
College  
Fort Leavenworth, Kansas**

**First Term AY 96-97**

Approved for Public Release Distribution is Unlimited

**DTIC QUALITY INSPECTED 3**

19970506 034

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE <i>09/12/96</i>	3. REPORT TYPE AND DATES COVERED MONOGRAPH	
4. TITLE AND SUBTITLE <i>CZW: A Battlefield Operating System for Force XXI?</i>			5. FUNDING NUMBERS	
6. AUTHOR(S) <i>MAJ STEPHEN M. WOOLWINE</i>				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) School of Advanced Military Studies Command and General Staff College Fort Leavenworth, Kansas 66027			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Command and General Staff College Fort Leavenworth, Kansas 66027			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT <i>Approved for public release; distribution unlimited</i>			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) <i>See Attached</i>				
14. SUBJECT TERMS <i>COMMAND AND CONTROL WARFARE C2 ATTACK C2 PROTECT</i>			15. NUMBER OF PAGES <i>50</i>	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	

## ABSTRACT

C2W: A BATTLEFIELD OPERATING SYSTEM FOR FORCE XXI? by MAJ Stephen M. Woolwine, USA, 50 pages.

This monograph examines the possibility of establishing C2W as Battlefield Operating System (BOS) for Force XXI. It focuses on emerging doctrine for C2W and Force XXI operations in order to evaluate the contribution of C2W in military operations of 2010.

The monograph begins with an examination of the BOS concept of BOS and its evolution U.S. Army doctrine. Understanding the systems approach to military operations provides the basis for discussion concerning the need to identify C2W as a critical function for Force XXI operations. At this point, the monograph describes the five elements of C2W: OPSEC; military deception; PSYOP; EW; and physical destruction and their application in the offensive and defensive forms of C2W.

With an understanding of the BOS concept and the concept of C2W established, the five battle dynamics of Force XXI operations are discussed. The five dynamics of battle command, battlespace, depth and simultaneous attack, early entry, and CSS provide a framework from which the U.S. Army will address expected condition changes for future war. These battle dynamics form the criteria for determining the feasibility of establishing C2W as A BOS for Force XXI.

The monograph then studies the application of C2W using two case studies, Operation Desert Storm and the CALL BCTP database to gain insight into the successes and failures. Based on the five battle dynamics of Force XXI and the two case studies, the monograph concludes with a discussion of establishing C2W as a BOS for Force XXI.

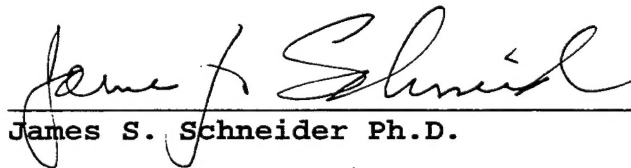
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

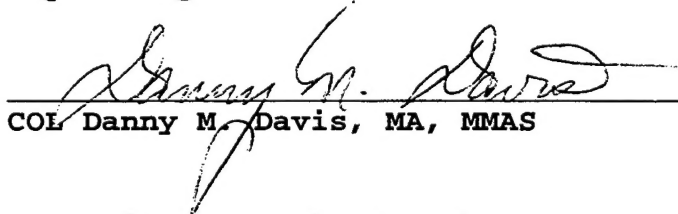
Major Stephen M. Woolwine

Title of Monograph: C2W: A Battlefield Operating System for  
Force XXI?  
\_\_\_\_\_

Approved by:

  
James S. Schneider Ph.D.

Monograph Director

  
COL Danny M. Davis, MA, MMAS

Director, School of  
Advanced Military  
Studies

  
Philip J. Brookes, Ph.D.

Director, Graduate  
Degree Program

Accepted this 20th Day of December 1996

## ABSTRACT

C2W: A BATTLEFIELD OPERATING SYSTEM FOR FORCE XXI? by MAJ Stephen M. Woolwine, USA, 50 pages.

This monograph examines the possibility of establishing C2W as Battlefield Operating System (BOS) for Force XXI. It focuses on emerging doctrine for C2W and Force XXI operations in order to evaluate the contribution of C2W in military operations of 2010.

The monograph begins with an examination of the BOS concept of BOS and its evolution U.S. Army doctrine. Understanding the systems approach to military operations provides the basis for discussion concerning the need to identify C2W as a critical function for Force XXI operations. At this point, the monograph describes the five elements of C2W: OPSEC; military deception; PSYOP; EW; and physical destruction and their application in the offensive and defensive forms of C2W.

With an understanding of the BOS concept and the concept of C2W established, the five battle dynamics of Force XXI operations are discussed. The five dynamics of battle command, battlespace, depth and simultaneous attack, early entry, and CSS provide a framework from which the U.S. Army will address expected condition changes for future war. These battle dynamics form the criteria for determining the feasibility of establishing C2W as A BOS for Force XXI.

The monograph then studies the application of C2W using two case studies, Operation Desert Storm and the CALL BCTP database to gain insight into the successes and failures. Based on the five battle dynamics of Force XXI and the two case studies, the monograph concludes with a discussion of establishing C2W as a BOS for Force XXI.

## TABLE OF CONTENTS

CHAPTER 1: Introduction.....	1
CHAPTER 2: The Battlefield Operating Systems.....	3
CHAPTER 3: What is C2W?.....	6
CHAPTER 4: Force XXI Battle Dynamics.....	18
CHAPTER 5: Historical Examples of C2W Successes and Failures.....	25
CHAPTER 6: Application of Criteria/Conclusion.....	37
Endnotes.....	42
Bibliography.....	45

## **CHAPTER 1**

### **INTRODUCTION**

TRADOC Pam 525-5 provides a conceptual framework for future Army operations in the twenty-first century. This framework describes a knowledge-based force capable of assessing large volumes of information in order to provide situational development, assessment of the situation, and the appropriate direction of military action. The document discusses five battle dynamics that will guide the development of this future force.<sup>1</sup> The battle dynamics are battle command, battle space, depth and simultaneous attack, early entry, and combat service support. Information technology will significantly impact three of the five battle dynamics of Force XXI: battle command, battle space, and depth and simultaneous attack. A key determinant in future Force XXI operations will be the ability to maximize information dominance while at the same time denying or degrading the information capability of the enemy. Thus, the purpose of this monograph is to determine the feasibility of establishing Command and Control Warfare as a Battlefield Operating System for Force XXI.

TRADOC Pam 525-69 provides the operational concept for how information operations are to support Force XXI operations. It provides insight into the important role information operations contribute to execution of battle command, battlespace dominance, and the application of deep and simultaneous attack in Force XXI operations. It describes the concept of command and control warfare (C2W), as the military strategy for implementing information warfare. The pamphlet stresses the need for integration of

information operations to ensure that they adequately support the commander's intent and concept of the operation, but provides little guidance on how to best do this.

C2W combines five primary components of operational security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction to reduce an enemy's ability to command and control while protecting the Army of the twenty-first century's ability to command and control. There is little debate currently on the importance of C2W/IW in the twenty-first century. The issue is how to best integrate C2W to support this force.

Throughout the evolution of warfare, military forces have attempted to increase the control of their own forces in relation to that of an adversary. Napoleon developed organizational changes, through the development of the corps and division, to enhance the control of his mass army. During the Civil War, commanders exploited the telegraph as a tool for control of forces on the battlefield. These efforts in developing control techniques have been much the result of the dispersed battlefield created by the increased lethality of weapons systems. The concept for Force XXI continues this effort in control on the dispersed battlefield through digitization and the development of the Army Battle Command System (ABCS). C2W retains considerable potential to complement these further efforts to exact control on the dispersed battlefield.

Individually, the five components of C2W have suffered considerable neglect in past planning. This will be unacceptable in an environment where information dominance is likely the key to success. C2W is much too critical to Force XXI operations to assume a business as usual approach to the application of its functional



elements. It must be integrated in Force XXI operations at the outset of the decision making process to take advantage of its possibilities.

The proposed methodology for the monograph is first to gain insight concerning the concept of the Battlefield Operating Systems(BOS). The next portion of the monograph will study the five pillars of C2W as well as their synergistic application. With a base of knowledge on C2W developed, the requirements generated by the five battle dynamics within Force XXI will be determined. The monograph will then study past applications of the elements of C2W to gain insight into the reasons for their success or failure. Finally, using the battle dynamics of Force XXI as criteria, the monograph provides an assessment on the establishment of C2W as a BOS for Force XXI.

## **CHAPTER 2**

### **THE BATTLEFIELD OPERATING SYSTEMS**

The term Battlefield Operating Systems (BOS) first appeared in The Army's keystone manual, FM 100-5, Operations, in 1993. This document defines BOS as :

"the major functions performed by the force on the battlefield to successfully execute Army operations (battles and engagements) in order to accomplish military objectives directed by the operational commander; they include maneuver, fire support, air defense, command and control, intelligence, mobility and survivability, and combat service support."<sup>2</sup>

The Commander views and synchronizes complex military operations in terms of these functional systems. At the tactical level of war, BOS enable a commander to

comprehensively examine “the integration, coordination, preparation, and execution of successful combined-arms operations.”<sup>3</sup>

BOS provide the commander a tool by which he is able to synchronize operations in time and space to achieve the desired effect. The seven functions interact to produce a set of conditions. Through the manipulation of the application of the individual functions in terms of time and space, the commander is able to produce a desired set of conditions. The functions act as enablers for each other. For instance properly synchronized fires are of considerable aid to the maneuver function, just as intelligence is a significant enabler for the fires function.

A clear indication of the importance of the BOS is the attention they receive in the Army’s Tactical Decision Making Process, specifically within the wargaming step of the process. During wargaming, the BOS are synchronized to maximize their application against an enemy’s most likely course of action. The enemy’s course of action is broken into events over time. Each BOS is applied and synchronized for each enemy event in time ensuring each is mutually supportive and that the desired effects on the enemy are met for each event.

Simply put, BOS allow the commander to view the complex world of military operations using an organic systems approach. The sum of the seven functions having a greater value than the individual parts. By adequately maximizing the contributions of each of the seven functions holistically, that is using each function to better enable the others, the commander is able to gain maximum output from resources allocated.

Peter Senge in his The Fifth Discipline provides excellent reasoning into the benefits of systems thinking that relates very well to the theory behind the BOS. In the opening pages of this work Senge uses a rainstorm to describe systems thinking.

A cloud masses, the sky darkens, leaves twist upward, and we know that it will rain. We also know that after the storm, the runoff will feed into the groundwater miles away, and the sky will grow clear by tomorrow. All these events are distant in time and space, and yet they are all connected within the same pattern. Each has an influence on the rest, an influence that is usually hidden from view. You can only understand the system of a rainstorm by contemplating the whole.<sup>4</sup>

This rainfall metaphor fits very well in understanding the concept of BOS. If one replaces the rainstorm with military operations, then the BOS become the clouds, rain, runoff and so forth. Each of the BOS react together over time and space to produce conditions (rainstorm) within a military operation. If any of the BOS are neglected or overemphasized in relation to the others, the expected end state is greatly threatened. The BOS must work together in a balanced and harmonious manner to be effective.

It could be argued that BOS are only a "fad" within the Army, as a result of their just recent appearance in FM 100-5. However this argument is likely dissipate into one of semantics, as the manual has seen other terms in its place over the years. The 1982 and 1986 versions preferred to use the term functions instead of BOS. The application of the differing terms were similar in effect however. Each to be used by a commander to coordinate and synchronize in military operations. Additionally, the Army Combat Training Centers began use of the term BOS in their AAR's in the early 1980's.

Regardless of the term used to describe the elements in the future, there will remain a number of critical functions that the Army must perform in order to conduct

successful military operations. This argument is best dealt by viewing an army as a living system. A living system, such as the human body, must perform a few critical functions for survival such as breathing, eating, and hydrating. The Army of the future will be no different, it will retain some number of critical functions to ensure its successful survival. The term currently in use in Army doctrine for these critical functions is BOS, as a result this monograph will adopt this term in its study of the potential impact that C2W will have on Army Force XXI Operations.

### CHAPTER 3

#### WHAT IS C2W?

C2W is the integrated use of psychological operations (PSYOP), military deception, operations security, operations security (OPSEC), Electronic Warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities.<sup>5</sup>

The tendency today is to confuse the terms C2W and Information Warfare. C2W is the military application of Information Warfare (IW), and as a result is a subset of IW.<sup>6</sup> To further clarify the situation, IW is part of the **national strategy** “to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one’s own information, information-based processes, information systems, and computer-based networks.”<sup>7</sup> C2W is the **military strategy** to create an information advantage by focusing on the C2 decision making process of both friendly and adversarial forces.

The concept of C2W is applicable throughout the strategic, operational, as well as tactical levels of war, although this monograph will focus on its application at the tactical

level. C2W is also applicable throughout the spectrum of military operations ranging from combat operations to operations other than war, and exhibits both offensive and defensive characteristics. Its application allows the commander to establish advantageous conditions for exploitation in military operations.

In essence, "C2W provides the commander with the means to achieve agility by focusing attacks on the adversary's ability to ability to command and control his forces while simultaneously protecting friendly C2. If adversary forces cannot act or react in a cohesive manner, friendly forces gain a comparable measure of agility... thinking, planning, communicating and acting faster than the enemy can effectively react."<sup>8</sup>

The components of C2W are not new, however the environment they operate in certainly is. Sweeping developments in information technology have produced increased capabilities to collect, process, analyze, and disseminate information. As a result, commanders have an increased ability in the timely and effective control of their forces. However, technology has also produced increased capabilities to attack this control as well. A more important change from the past, however, is C2W's synergistic application of the five components creating a significant force multiplier for the commander. The tools of C2W have existed for ages, but the toolbox to carry them all in only recently arrived.

Application of C2W does not necessarily require the application of all five elements simultaneously. The situation and military operation at hand may only require the application of one or two of the elements. What is most important is that these elements be applied in a complementary and synergistic manner to produce the desired

conditions. Clausewitz describes the principle objective in warfare as the conquering and destruction of the armed forces of the enemy. This action becomes much simpler and less costly in lives and materiel if the enemy has been made unable to control these forces through the application of the following five elements of C2W.

### PSYOP

PSYOP are defined as operations to “convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals.”<sup>9</sup> The goal of these operations is to produce or reinforce attitudes and behavior that will create favorable conditions for the attainment of friendly objectives.

PSYOP are extremely useful in support of the C2W concept. They allow a friendly commander to communicate directly with his adversary in an effort to target his behavior (command and control). They provide the commander the ability to get information to people in denied areas which can be useful in a wide range of military operations. PSYOP can enable the commander to reduce the will of an adversary to fight while at the same time enhancing the morale of his own force. Desert Storm proved that PSYOP was quite useful when applied in conjunction with attack missions to communicate to an adversary the alternative to combat (surrender). Lastly, PSYOP are quite useful in support of military deception, as it allows for the direct reinforcement of behavior produced by the deception plan.

An important fact to remember concerning PSYOP is that the message conveyed to the adversary must be based on facts that the adversary can confirm with his own

resources. The message should also show consideration for perceptions and tendencies of the target. If PSYOP delivers a message that is not believed or friendly forces cannot deliver the stated or implied threat, the effectiveness of PSYOP is lost. As a result, maintenance of credibility and synchronization with the operational plan are paramount in PSYOP.

### OPSEC

OPSEC focuses on denying critical elements concerning friendly forces from a potential adversary. By denying an adversary these critical pieces of information, the commander forces him to make decisions and take action based on limited intelligence. This in effect produces faulty decisions and will also likely increase the time taken by the adversary to make the decisions.

The planning process for executing an effective OPSEC program occurs in three phases. The first phase is for planners to determine friendly actions or indicators that will lead an adversary to determine current and future friendly courses of action. The second phase is to assess the adversary's intelligence collection apparatus to determine which of the aforementioned indicators he may be able to collect. Lastly the commander must determine what action he will take to deny or suppress his vulnerabilities.<sup>10</sup>

The Information Age has significantly increased the challenge for OPSEC. Of particular note is the impact that the commercial media has on military operations. Certainly in the area of deterrence the media can be very helpful. By providing coverage of the deployment of a Deployable Ready Brigade (DRB) into a theater of operation, the press displays American readiness and commitment to its national interests. The

problem arises when the media is present in an actual area of operation and capable of real time reporting. It becomes extremely important at this point that the commander use the utmost judgment and analysis in allowing press coverage. Close coordination is necessary between OPSEC planners and Public Affairs personnel to prevent the disclosure of critical operational information. This close coordination is also useful in developing the appropriate operational snapshot that is delivered an adversary.

Instruments of OPSEC operations include: the use of counterintelligence assets to deny adversarial human intelligence HUMINT; Information Security (INFOSEC) to prevent unauthorized access or manipulation of information systems; and Communications Security (COMSEC) to protect friendly telecommunications systems. The PSYOP and Deception elements of C2W can also contribute in the OPSEC arena by confusing or altering the appearance and of friendly OPSEC vulnerabilities.

### MILITARY DECEPTION

Military deception as defined in FM 100-5, Operations “are designed to mislead enemy decision makers by distorting, concealing, and falsifying friendly intentions, capabilities, and dispositions.”<sup>11</sup> The goal is to cause a change in the enemy’s behavior in a way that is exploitable by friendly forces. Deception ultimately provides the friendly force with the advantage of surprise in enemy operations. It supports the commander’s application of economy of force and also facilitates mass at the decisive point.

Deception targets the perception of the adversary. By manipulation or distortion of force capabilities and disposition, the friendly commander attempts to deliver erroneous signals to the adversary to alter or enhance his perception of friendly force



capabilities and intentions. The deception plan most likely to succeed exploits an adversary's predispositions. If the adversary is delivered a deception plan that lays out events as he would expect based on predisposed beliefs concerning friendly capabilities and tendencies, the plan has a significant chance of succeeding. "If deception targets tend to perceive what they expect, then these expectations furnish leverage to a deception plan--a form of mental jujitsu."<sup>12</sup>

There are five major components of battlefield deception:

Objective: What action is desired of the enemy? The objective may be to convince the adversary he is numerically inferior or that he faces an opposing main effort when in fact it is only the supporting effort.

Target: The target for the deception operation is the enemy decision maker. It does little good to target a commander with a deception effort he does not retain decision making authority to produce the desired objective.

Story: What is to be portrayed for the adversary to produce the desired objective? Otherwise known as the "big lie" to be told the enemy decision maker.

Plan: The deception plan details the assets and methods to be applied to create the story. It provides the concept of how the story is to be delivered.

Event: The specific actions to be taken to provide enemy intelligence collection assets with faulty indicators.<sup>13</sup>

Other considerations in deception planning include the enemy's collection capabilities and receiving feedback on the effectiveness of the deception plan. Deception indicators that fall on deaf ears are obviously ineffective. Additionally, the deception

plan must allow for responsive feedback as to the extent the adversary has taken the “deception bait”. Including deception related Priority Intelligence Requirements (PIRs) in the operational plan will satisfy this need.

### ELECTRONIC WARFARE

Electronic Warfare (EW) is defined as “any military action involving the use of the electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.”<sup>14</sup> EW is divided into three principle divisions, electronic attack (EA), electronic protect (EP), and electronic support (ES). Each of these divisions are capable of making significant contributions to the overall C2W effort.

Through the application of lethal (directed energy weapons and anti-radiation missiles) and nonlethal (jamming) means, EA degrades, denies, or destroys an adversary’s use of the electromagnetic spectrum. Additionally, EA allows for the exploitation of an adversary’s use of the electronic spectrum through the application of electronic deception.

EP protects personnel, facilities, or equipment from the effects of friendly or enemy EW which degrades or destroys friendly communications and non-communications capabilities.<sup>15</sup> The major effort within EP is management of friendly emanations to protect against an adversary’s attempts to locate and target friendly communications and non-communications systems. Frequency management of the electromagnetic spectrum will also contribute to EP.

ES gathers information by intercepting, locating, and exploiting enemy communications and non-communications systems.<sup>16</sup> It provides the friendly

commander with near real time combat information concerning an adversary's C2 posture on the battlefield, as well as possible insight related to the adversary's intent.

### PHYSICAL DESTRUCTION

Physical destruction describes the "application of combat power to destroy or neutralize enemy forces and installations."<sup>17</sup> Within the realm of C2W, physical destruction may be used to permanently shut down or temporarily degrade adversarial C2 capabilities in support of the overall C2W concept. Clearly the predominance of the targets would likely be C2 nodes within the concept, however physical destruction could also be applied in support of the other pillars of C2W.

Careful analysis is required in applying physical destruction to ensure that the criticality of destruction is weighed against the intelligence gained from the target's survival. Timing of physical destruction is also critical, as the adversary may be able to reconstitute the target's capabilities, and premature destruction would have limited overall effect. Additionally, destruction assets will likely be limited, and as a result targets will require analysis to determine those that require destruction versus those that will only require degradation through the other pillars.

### C2 Attack

C2W, as mentioned previously in the introduction, has offensive as well as defensive applications. The offensive application of C2W is described as C2 attack. Through the application of C2 Attack a friendly force is capable of denying an adversary information through the influencing, degrading, or destroying his C2 systems.<sup>18</sup> The ultimate goal of C2 attack is to prevent effective adversarial application of military

power. This results from forcing the adversary to make and execute decisions in a military environment with outdated, inaccurate, or distorted information and degraded resources for the acquisition, processing, analysis, and dissemination of information.

Three main principles provide the framework for the application of C2 Attack. The first being, in order to plan effectively C2 Attack, planners must have an in-depth understanding of the operational plan. With this understanding, planners are then able to effectively synchronize C2 Attack operations to set the desired conditions for execution. The last principle addresses the importance of aggressively seizing and maintaining the initiative by attacking the adversary's information systems. Through these attacks on his information systems, the adversary is forced to become reactive in his decisions and actions. As a result of becoming reactive, the adversary is forced to slow his tempo. He lacks the information necessary to be forward looking. The adversary no longer is capable of effective application of combat power at the proper time and place, as the system to execute control of these functions has been degraded.<sup>19</sup>

Effective application of these C2 Attack principles produces four main effects on military operations. First, it denies the adversary information by disrupting his observation and degrading his decision formulation.<sup>20</sup> The effective application of OPSEC obviously plays a fundamental role in denying an adversary information however, PSYOP and Deception can also support in this effort. Deception attempts to induce the adversarial commander to deploy his forces in an inappropriate manner in relation to friendly operations. It is also extremely useful in overloading the intelligence

collection process of the adversary with erroneous and conflicting data. This places the adversary in the unenviable position of determining truth versus fiction.

Secondly, C2 Attack's manipulation of perception creates disorientation in the adversary's decision cycle.<sup>21</sup> Deception is the key pillar in producing this effect. By hiding the real and displaying the false, the adversary is forced into making inappropriate decisions. Additionally, deception also assists in conditioning the adversary to patterns of friendly operations that can be exploited in the future.<sup>22</sup> PSYOP is also extremely effective in reinforcing these adversarial perceptions. OPSEC certainly plays a supporting role in this area as well, in that it allows for the hiding the real portion of the distorted picture. Physical destruction assists in manipulating perception by denying an adversary the capability to observe the "real". EW contributes in a similar manner, denying the communication means for the transfer of information to disprove the misperception.

C2 Attack also produces the effect of severing or degrading the flow of information between an adversarial commander and his subordinates.<sup>23</sup> EW and physical destruction are most effective in creating this effect. Great care must be taken to weigh efforts in this area against those involved in manipulating perception. Degradation or destruction of the means for a commander to communicate his guidance and intent could negatively impact efforts in manipulating the adversarial commander's perception. No need to change his perception if the means to transfer this perception to his subordinates is removed. PSYOP is also quite useful in this effort through attempts to discredit the adversarial leadership amongst its forces.

Lastly, C2 Attack allows application of physical destruction to neutralize or destroy adversarial information capabilities.<sup>24</sup> As mentioned previously, an adversary may possess the capability to reconstitute a C2 capability to a certain degree. Consequently, the timing of C2 Attack must be closely synchronized to maximize the exploitation of a degraded, disrupted, or destroyed adversarial C2 capability.

### C2 Protect

C2 Protect is “the maintenance of effective C2 of ones own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C2 system.”<sup>25</sup> In C2 Protect, the adversary’s C2 Attack capabilities are analyzed to develop possible C2 Attack COA’s against our own C2 systems. In effect our own C2 systems are viewed through the eyes of the enemy to determine critical vulnerabilities. These vulnerabilities will likely drive the enemy’s C2 Attack COA. Based on this likely enemy COA, friendly forces are able develop a C2 Protect plan to defeat or minimize its effectiveness.

As with C2 Attack, there are a number of principles to guide the commander in developing his C2 Protect plan. The first is the critical importance of gaining C2 superiority. This allows for friendly forces to maintain the exchange of information to and from subordinates allowing for effective decision making. It is also important that an effort be made to reduce the enemy’s C2 Attack capabilities, while at the same time reducing friendly C2 Attack vulnerabilities. Lastly effective management of the Electromagnetic Spectrum is required to prevent friendly interference of our C2 systems.<sup>26</sup>

OPSEC plays a critical role in the C2 Protect aspect of C2W. Effective OPSEC operations will greatly assist in the denial of an adversary the critical information he needs to make effective operational decisions. OPSEC planning can identify critical indicators of friendly intentions that an adversary would apply in making these operational decisions. It will also provide for actions to be taken to deny these indicators to the adversary.

The PSYOP pillar of C2W can also be of significant value in the C2 Protect role. Through PSYOP a friendly commander can counter enemy propaganda, as well as adversarial media attacks. PSYOP can also provide legitimacy to friendly operations, as well as attempt to drive a wedge between the adversarial commander and his forces. In the protection role, PSYOP is also useful in attempting to persuade an adversary that the military capabilities of friendly forces are far superior, and further confrontation will lead to significant loss to the adversary.

Through deception operations, friendly C2 capabilities can also be protected from enemy C2 Attack. Deception allows a friendly commander to mislead an adversary as to his true C2 disposition, thereby protecting friendly C2 systems and causing the adversary to ineffectively commit C2 Attack assets.

In the EW arena, ES can provide information from SIGINT as to the intent of enemy C2 Attack operations. This allows for further C2 Protect actions to be taken by the friendly commander. Additionally EA can be applied to deny information required for C2 Attack operations, as well as to defeat actual enemy C2 Attack attempts.

Physical destruction of an adversary's C2 Attack resources clearly contributes to an effective friendly C2 Protect operation. By identifying these resources through intelligence collection, the friendly commander is able to defeat them prior to their application against his C2 systems.

### Summary

To summarize the strategy of C2W, the commander must protect the command and control of his own forces while making every effort to deny, deceive, disrupt, and if required, destroying the C2 capability of his opponent. The goal is to operate inside the enemy's decision cycle, wresting away the initiative and forcing the enemy into operating in a reactive manner. Without effective command and control, adversarial commanders are forced into autonomous operations. This greatly reduces their capability to achieve synergistic effects, and as a result reducing their efforts to piecemealed uncoordinated operations.

## **CHAPTER 4**

### **FORCE XXI BATTLE DYNAMICS**

To address the changing conditions for future war, TRADOC Pam 525-5 describes a framework of five battle dynamics. Each of these battle dynamics is reflective of the five major areas of change related with the future nature of warfare. To assess its contribution to Force XXI operations, C2W must be measured by its ability to address projected change within these five dynamics.

These five battle dynamics include battle command, battlespace, depth and simultaneous attack, early entry and combat service support (CSS).<sup>27</sup> In an effort to gain



insight as to how these dynamics frame the future battlefield, it is now appropriate to study each dynamic individually beginning with battle command.

### Battle Command

Battle command is the “art of battle decision making, leading and motivating soldiers and their organizations into action to accomplish missions.”<sup>28</sup> It is the process through which a commander visualizes a situation, assesses the conditions, and directs appropriate military action. This demands of this dynamic will be greatly change on the future battlefield.

The Force XXI battlefield is projected to differ from the contemporary in terms of scope, intensity, and tempo. These differences will result from the increased range, precision, and lethality of weapons combined with the timeliness and accuracy of information provided by information age technology. The dynamic of battle command must address these challenges.

The centerpiece for battle command in Force XXI will be the Army Battle Command System (ABCS). Through advances in information technology, the ABCS will broadcast battlefield information, as well as information from other sources, and integrate that information, including real-time friendly and enemy situations, into a digitized image that can be graphically displayed in increasingly mobile and heads-up displays.<sup>29</sup> This process will provide the commander with accurate and timely battlefield information , allowing him to make and execute decisions at a faster pace than an adversary.

ABCS will produce for the commander a relevant common picture of the battlefield to include friendly as well as enemy situations. This digitized system will significantly increase the tempo of future operations, as it allows for the instant communication of battlefield information. Through the common situational awareness a commander will be capable of more rapid synchronization, allowing him to focus rapidly his combat power at the decisive point and time. Changes in the operational situation or new operational orders will be instantly broadcast to units, avoiding slower radio or liaison means. Additionally the chance for misinterpreting intent will be reduced as the delivery system is direct.

ABCS will also connect a commander with his combat support (CS) and combat service support (CSS) elements as well. This will allow for this first time, direct connectivity between a commander and his CS/CSS elements, greatly easing his requirement to ensure their synchronization into his operation.

The increased battlespace associated with Force XXI operations will put great demands on battle command. Without the instantaneous communications and common situational awareness of ABCS, the Force XXI commander's ability to "control" his battlespace are significantly reduced. Consequently, ABCS will require a commander to exercise effective electromagnetic supremacy in the conduct of all military operations. Failure to do so, could result in the denial of the spectrum for use by the ABCS. To achieve the information advantage, and as a result the increased tempo, called for in Force XXI operations, the commander must continually consider protection of his own use of the spectrum, while at the same time denying or exploiting its use by an adversary.

Because of the increased flow of information associated with the ABCS, it is quite possible that the organizational structures within the Army could flatten. Reduction in the levels of command produces an increase in importance in the securing of spectrum supremacy to support ABCS. If there are fewer decision makers on a more dispersed battlefield than today, their linkage becomes much more critical.

### Battlespace

Battlespace describes the ability of a commander to visualize his the area of operations and the way that forces will interact within it. The dimensions of battlespace are greatly effected by the mission, enemy, terrain, troops, and time available (METT-T). However, in basic terms a commander's battlespace is largely determined by his capabilities to acquire and engage an adversary. The significant change projected within this battle dynamic is that a commander's battlespace will greatly expand in future operations.<sup>30</sup>

As discussed previously, the dynamics of battle command and battle space are closely linked. The concept of battle command provides for the control and dominance of one's battle space, and the increased dimensions and demands of one's battlespace produce increasing demands on battle command.

To produce dominance of battlespace required in future warfare, Force XXI will rely on an increased tempo within the battlespace in terms of speed, space, and time. The Army of Force XXI will dominate an adversary with quicker actions, over a greater distance, and with greater efficiency. The tool to achieve this quantum leap in tempo will be the power of information.<sup>31</sup>

Certainly information alone will not provide the Force XXI commander with all that is required to dominate his battlespace. Increases in weapon technology will certainly increase the combat power of this future commander as well. The problem is that the this increase in combat power also brings with it an increase in battlespace. This produces a situation in which information can make a significant contribution. With an increase in the availability of information, the commander is better able to determine effectively situations suitable for economy force application. Resulting in his ability to better apply combat power at the decisive point and time. The situational awareness within battle command will provide this capability.<sup>32</sup>

It is not just the quantity or quality of the information available on the Force XXI battlefield that will produce success, but the speed at which it is delivered as well. It has often been said, intelligence that does not reach the commander in time to make an effective decision is merely history.

In the time of Napoleon, information moved at the same rate as the enemy (the speed of horseback)! During Desert Storm, a large amount of high quality of national level intelligence products were available to lower level commanders. However, limited dissemination capabilities reduced its usefulness. With the digitization discussed in the battle command dynamic, this kind of information is to be available to the tactical commander upon its entry into ABCS. The speed of information exchange through ABCS will significantly decrease the time of dissemination. This puts more time in the hands of the commander to make a decision on action, which should directly contribute to his dominance of battlespace.

### Depth and Simultaneous Attack

Within the dynamic of depth and simultaneous attack, the Force XXI commander will have the capability "to directly influence the enemy throughout the width, height, and depth of his battlespace to stun, then rapidly defeat an enemy."<sup>33</sup> Through depth and simultaneous attack an adversary is overwhelmed with a number of military actions throughout the depth of his sector. These military actions include combine the use of short and long range precision fires as well as the application of information warfare in an effort to blind and demoralize an enemy, concurrent with rapid combined arms maneuver (ground and air).<sup>34</sup>

Critical to the application of this dynamic will be precision target identification, but not in merely an accurate target location. For attacks to be effective throughout the depth of the battlefield, an adversary must be understood from a systems point of view. Key nodes and vulnerabilities must be identified and attacked to produce the paralysis desired. "If we can plan and conduct simultaneous attacks throughout the depth of every sector to destroy, disrupt and control the threat information flow--if we can concurrently protect friendly capabilities to gather, generate, and rapidly distribute information throughout the force and act upon it--we can attain decisive victory."<sup>35</sup>

### Early Entry

The dynamic of early entry addresses the necessity for units in Force XXI to "...deploy rapidly, enter the operational area, secure the lodgment, and either immediately have decisive effect...win the first battle...or create conditions for the arrival of substantial follow on forces that then conduct decisive operations."<sup>36</sup> This early entry

force of Force XXI will be one built on modularity and capable of tailoring itself to satisfy METT-T requirements.

The first goal within the dynamic of early entry is the simultaneous application of force or control throughout the operational area. The concept of force projection is brought to full fruition within this dynamic. There will be a number of tethers between the early entry force and its homestation(s). These will include intelligence, C2, as well as logistical support links. These tethers will be active at homestation, enroute to a theater of operations, and in the theater to provide the information requirements to the early entry force.

To enhance the dynamic of early entry the Army of Force XXI will have the ability to rehearse operations using simulations. Simulation will allow for units separated geographically to rehearse together prior to entry. Multispectral imagery, accurate weather forecasts, and up to the minute intelligence concerning the theater of operations will provide realism to the conditions within these rehearsals.<sup>37</sup>

#### Combat Service Support

The dynamic of CSS will experience considerable change under the Force XXI concept. At the tactical level these changes will be much the result of the common situational awareness discussed previously in the dynamic of battle command. CSS leaders armed through ABCS with the needs of a supported force, will push forward required supplies. Eliminating a considerable portion of the requisition process.

Common situational awareness will not only allow for the timely and accurate delivery of supplies, but will allow the CSS leader to quickly realize changes in the

operational situation, requirements, and priorities. This will provide him with an enhanced capability to effectively redirect resources to assist the supported commander maintain the operational tempo required in the Force XXI environment.

Armed with an understanding of the Army framework to address change in the military operations of Force XXI, it is now appropriate to study past applications of C2W to evaluate successes and failures. This will allow for measuring the effectiveness of C2W in recent military operations and and determine related causes.

## **CHAPTER 5**

### **HISTORICAL EXAMPLES OF C2W SUCCESSES AND FAILURES**

Because the concept of C2W entered Joint and U.S. Army doctrine within the past year, it is extremely difficult to identify case studies suitable for studying the sources of its success or failure. As a result, one is often forced to study the application C2W in terms of its individual elements. Even when forced to take this approach, evidence of interconnectivity within the application of the individual elements is still found.

The concept of C2W owes its evolution to Operation Desert Storm, and as a result this joint operation provides an excellent case study in the application of the elements of C2W. An effective outlet through which to study the application of the elements of C2W within the US Army, is After Action Reviews (AARs) from the Battle Command Training Program (BCTP) database maintained by the U.S. Army's Center for Lessons Learned (CALL). Together these sources of information provide considerable insight into the reasons for success or failure in the application of the elements of C2W.

## Desert Storm

The extent that coalition forces were able to degrade Iraq's command and control is best exemplified by the discussions that took place between Gen Schwarzkopf and Iraqi senior military officers at Safwan on 3 March. The leaders were together to finalize the cease-fire terms. After informing CINCCENT as to the status of Coalition Prisoners of War, the Iraqi leadership inquired as to the status of Iraqi POWs held by coalition forces. When Gen Schwarzkopf replied that preliminary numbers were in excess of 58,000, the Iraqi vice chief of staff appeared stunned. The Iraqi III Corps Commander, leader of Iraqi soldiers who had occupied the eastern half of the Kuwaiti-Saudi border and the Kuwaiti coastline, was asked if this was possible. The III Corps replied that it was possible, but he did not know. The discussion later turned to the establishment of a no-fire line to separate coalition and Iraqi forces. Upon CINCCENT's proposal for a line, the vice chief of staff inquired as to why it was drawn behind Iraqi troops. Gen Schwarzkopf replied that the line represented the forward line of the coalition advance. Again the III Corps commander replied that it was possible, but he did not know. Three days after the end of hostilities, the Iraqi leadership still were ignorant to the number of soldiers they had lost and where coalition forces were.<sup>38</sup> That is about as good as it gets in denying an adversary the ability to command and control his forces.

This C2W effort was executed without established doctrine or guidelines to follow. The lessons learned in the application of the separate elements of C2W provided the basis for the development of the overall C2W concept. As a result, a study of their



application during this operation provides considerable insight into the capabilities and expectations associated with C2W.

### Deception

The goal of the coalition deception plan was to convince Iraq that the main attack would be launched directly north into Kuwait, supported by an amphibious assault along the eastern Kuwaiti coast. This would divert Iraqi forces away from the coalition main effort in the west, and cause Iraqi forces in the east to become fixated on the Kuwaiti coast.<sup>39</sup>

The deception plan was a clearly a joint effort. Prior to the initiation of the air campaign, air elements conducted air refueling and training to desensitize the Iraqis to the preparations necessary to start the campaign. Additionally, during the actual air campaign targets in the west received reduced attention until just prior to the initiation of the ground war.

Naval forces conducted a number of feints and demonstrations in the northern Persian Gulf to reinforce Iraqi perceptions that the main effort would attack directly north into Kuwait. The positioning of a large amphibious task force (ATF) in the gulf also supported the deception effort.<sup>40</sup>

The US Marines and other ground forces south of Kuwait conducted raids in an effort to fix Iraqi divisions along the border between Saudi Arabia and Kuwait. As ground units moved into positions in the west for the main attack, the 1st Cavalry Division remained in the east to simulate the activities of the departed divisions. During the thirty days before the initiation of the ground war, the 1st Cavalry Division conducted

aggressive feints, demonstrations, and artillery raids against Iraqi defenses in western Kuwait. These actions by the 1st Cav Division supported the deception plan and fixed five Iraqi divisions in place, well away from the zone of attack of the main effort.<sup>41</sup>

### OPSEC

A stringent OPSEC program was in effect throughout the operation. At times the effort ran counter to the desires of many of the subordinate ground commanders. Ground reconnaissance in the main attack zone in the west was denied to prevent compromise of the plan and forced units to rely on echelons above corps (EAC) and national level intelligence assets. However, aggressive reconnaissance and counter reconnaissance efforts in the east was very effective in denying the Iraqis information on coalition dispositions and intent.<sup>42</sup>

As coalition forces built up south of Kuwait, Iraq responded with the deployment of additional infantry divisions. As the flow of coalition forces continued and allowed for their positioning in more westerly locations, Iraq responded with deployments to counter. As a result of this Iraqi response, Gen Schwarzkopf order no further coalition troop deployments to the west. Instead, he ordered them to deploy into basecamps in eastern Saudi Arabia. Also in support of the OPSEC effort, CINCENT decided against a proposal to use King Khalid Military City to build up near-term supplies, realizing a build-up in this vicinity could compromise the coalition plan.<sup>43</sup>

### PSYOP

An Iraqi Division commander following the cease fire, stated that after the air campaign the single greatest threat to his troops morale was coalition PSYOP. PSYOP

leaflets and radio broadcasts undermined unit morale, provided instructions on how to surrender, instilled confidence that prisoners would be treated humanely, and provided warning of impending air attacks encouraging desertion among Iraqi forces.<sup>44</sup>

To plan and monitor the execution of PSYOP, a PSYOP planning group was established with personnel from CENTCOM, Special Operations Command (SOCOM), and the US Army 4th PSYOP Group. The objectives for the PSYOP campaign laid out by this group were: gain acceptance and support for US operations; encourage Iraqi disaffection, alienation, defection and loss of confidence; create doubt in Iraqi leadership; encourage non-cooperation and resistance; strengthen confidence and determination of friendly states to resist aggression; and improve deterrent value of US forces.<sup>45</sup>

Leaflet, radio, and loudspeaker operations supported the PSYOP effort, with leaflet operations being the most common means of delivering the PSYOP message. In total, there were approximately twenty-nine million leaflets providing thirty-three different messages in the theater.<sup>46</sup> The themes delivered in leaflet operations had a building effect. Initial themes centered on stressing the need for peace and brotherhood, then transitioned to emphasis on enforcement of the 15 January UN deadline. With the initiation of the air campaign messages were delivered in an effort to exploit weapons effects to inform Iraqi forces they were targeted for bombing. Enemy Prisoner of War (EPW) interviews produced validation of the successful leaflet operations.<sup>47</sup>

The Voice of the Gulf radio network began broadcasts from both ground and aerial platforms on 19 January. The network was operational eighteen hours a day for

some forty days. Broadcasts were targeted against Iraqi propaganda, disinformation, and encouraged defection/surrender of Iraqi forces.<sup>48</sup>

Some sixty-six loudspeaker teams were deployed in the theater. The messages delivered by these teams were similar to those delivered by leaflet operations. A number of EPW's stated that they heard the loudspeaker broadcasts and surrendered for fear of further bombing.<sup>49</sup>

## EW

All three aspects of electronic warfare were well integrated and effective during the operation. However, of significant note was the coalition's EW efforts in the area of suppression of enemy air defense (SEAD). The airspace over Iraq was filled with jammers, shooters, and bombers. The ES and EA capabilities of coalition forces significantly degraded Iraqi air defense capabilities.

US Navy and Air Force platforms jammed early warning, acquisition, and ground control intercept (GCI) radars. Iraqi voice nets, data links, and navigational systems were also jammed. High Speed Anti-Radiation missiles (HARMs) were quite effective in destroying Iraqi radar systems. Surface to air missile (SAM) operators frequently chose to engage coalition aircraft without little or no radar guidance, significantly decreasing their effectiveness. This effective application of EW in support of SEAD operations combined with actions in the physical destruction element, greatly denied the Iraqi's the ability to control their air defense system.

## Physical Destruction

Coalition efforts in applying physical destruction against Iraq's command and control were quite impressive. A primary objective of coalition air planners was the isolation and incapacitation of the Iraqi regime. Contributing to the effectiveness of coalition efforts in this area was Iraq's centralized decision making and C2 process. This centralization had a crippling effect on Iraqi forces when critical command facilities were destroyed. Just the fear of attack kept Saddam Hussein away from his primary C2 locations, forcing him to use less capable means. This not only damaged his control of forces but forced him to use less secure means of communication, thereby supporting the coalition's intelligence collection operations.<sup>50</sup>

In addition to attacking key Iraqi command and control centers, coalition planners also attacked Iraq's civil telecommunications system. Through this system passed approximately sixty percent of military land line communications. This system was Saddam's preferred secure method of communicating, and its degradation deprived him of effectively command and controlling his field forces.

As early as mid-February, according to CENTCOM and EPW reports, only sporadic communications took place between corps and division headquarters and their subordinate units along the Kuwait-Saudi Arabia border. It seems that in many circumstances Iraqi commanders were forced to use messengers to communicate with higher, lower, and adjacent forces. From EPW reports it was determined that a number of Iraqi commanders had no communications whatsoever with their headquarters for more than a week for prior to the initiation of the coalition ground attack.<sup>51</sup>

Effective application of the element of physical destruction denied Iraqi commanders ability to control their forces. Additionally, it denied them critical vertical and horizontal transfer of information necessary for effective decision-making. This greatly allowed coalition commanders the ability to operate inside their enemy's decision cycle.

### BCTP Archives

Review of the BCTP archives reveals more failures than successes. The greatest source of failures are a result of poor planning and synchronization of the elements in support of the overall operational plan. Often the elements of C2W were not even addressed in the planning process. When the elements were included in planning they were often included as an afterthought, and as a result not well synchronized in support of the commander's operational concept.

In the area of OPSEC the biggest problem seems to be a lack of understanding as to the critical role essential elements of friendly information (EEFI). EEFI identifies the "critical aspects of a friendly operation, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation."<sup>52</sup> As discussed previously in the OPSEC element of C2W, EEFI must be the driving tool in the development of an effective OPSEC program. Review of BCTP AAR material reflects that often EEFI are not being developed, and when established they do not receive the necessary attention in the development of an effective OPSEC program. They become just another addition to the collage of charts hanging next to the situation map.

It becomes very difficult to evaluate OPSEC effectiveness when units struggle with the basics of EEFI development and application. The next step is to develop the countermeasures necessary to protect these elements. This is where the true test comes, managing and allocating resources to ensure to protect them. From the BCTP AAR data it would appear most Army units have barely left the gate in the race to develop effective OPSEC programs.

Deception has been identified as an Army wide weakness, based on BCTP observations.<sup>53</sup> Common threads identified within the element of deception include: failure to establish centralized command and control for the deception effort at division level; lack of believability in development of the deception plan; reactive instead of proactive planning of deception; and a tendency to neglect commitment of resources to support deception planning.

To execute effective deception efforts at the division and corps level, centralization of planning and C2 are absolutely critical. Someone must oversee the deception effort to ensure that subordinate efforts are in concert with the overall deception plan. On multiple occasions, observer controllers (OCs) commented that there was no one in the main command posts with the responsibility for tracking execution or assessing the effects of the overall deception effort.<sup>54</sup>

The tendency in deception planning seems to follow the principle of "pass the buck". That is for a division to assign a subordinate unit with the responsibility of planning and executing the deception operation. An excellent example of this occurred in Rotation 94-06 when Corps tasked the Division to support the deception effort, the

Division then tasked a Brigade with its responsibility, and the Brigade ended up tasking two teams to plan and execute the deception.<sup>55</sup>

The centerpiece for developing an effective deception plan, as discussed in chapter 3, is the plan must be believable by an adversary. To execute a deception operation that is not believable is a waste of effort and resources. During one rotation, a divisional cavalry squadron, with sixteen tanks, received the mission to replicate an Armored Cavalry Regiment without receiving additional combat resources.<sup>56</sup>

The most successful deception effort found in the archives, was developed from analysis of the most likely friendly course COA as seen from the adversary's standpoint. The friendly force used this COA to guide their deception planning, and then selected a suboptimal COA as the basis for developing their actual operational plan.<sup>57</sup> This unit used the adversary's conditioned perceptions, what the enemy expects in the form of a most likely friendly COA, to produce an effective deception operation. In addition, they also realized that their adversary would expect some sort of deception operation, and as a result executed a feint to satisfy this expectation.<sup>58</sup>

Deception planning must be developed in concert with the actual operational planning. This ensures that the deception plan is well synchronized and effectively supports the commander's operational plan. In many instances it appears that deception planning is done as an afterthought. The operational plan is developed and then planners decide a deception effort must be planned. Deception planning is not receiving the emphasis during the planning process that it demands to be effective.<sup>59</sup>



Related to the problems of believability and centralized C2 concerns, is the issue of allocating sufficient resources to support the deception effort. Units are not allocating sufficient resources to the deception effort.<sup>60</sup> Commitment of resources contributes directly to the believability problem. Without the adversary seeing the resources he would expect an opponent to deploy, a deception plan is doomed from the beginning. The lack of centralized planning has clear implications on this issue of allocating sufficient resources to the deception effort.

Another area in need of Armywide improvement, according to BCTP OCs, is the planning and execution of PSYOP.<sup>61</sup> Units are not effectively integrating PSYOP to support their operational plan. In one instance, a divisional SOP listed PSYOP under the staff responsibility of the G-5.<sup>62</sup> During another rotation PSYOP units were subordinated to the DISCOM, relieving the division staff from responsibility for planning and synchronizing the PSYOP effort.<sup>63</sup>

It also seems that the tendency is to task only PSYOP units with PSYOP related tasks. Rather than tasking brigades with support to the PSYOP effort, divisional orders tend to task only PSYOP units with this support.<sup>64</sup> This method of tasking seems only to further inhibit effective integration of PSYOP into operational planning.

It does not come as a surprise that the most effective integration of PSYOP to date was observed in the same rotation that produced the best deception effort. During rotation 94-07, the Divisional PSYOP Support Element (DPSE) was well integrated into the division staff. The DPSE was included in recurring briefings to the commanding general providing the commander with continuous updates as to the progress of the

PSYOP effort. Additionally, PSYOP was well integrated into the deception plan supplying the deception effort with leaflets and loudspeaker operations that enhanced the picture developed by actual forces portrayed within the deception effort.

Possibly the best indication of the lack of understanding for the role of PSYOP within the C2W concept is seen in the Final Exercise Report for rotation 96-07. In this report under the title of C2W, comments are made concerning the unit's application of deception, OPSEC, and EW.<sup>65</sup> Listed under a separate heading later in the report is a discussion of the unit's use of PSYOP.<sup>66</sup> This makes a clear statement as to the understanding of PSYOP and its application within a synergistic C2W effort.

Actions taken within the element of EW seem to be much better than that of OPSEC, deception, and PSYOP. A review of the archive materials reflects much better synchronization and integration of EW than the previous three elements discussed. The only real issue with EW seems to be the balancing of jamming efforts (EA) versus that of collection (ES).<sup>67</sup> Otherwise, it appears that units have been quite effective in coordinating and synchronizing the EW effort with that of the operational plan.

Feedback concerning the physical destruction element of C2W also appears to be positive. Units are effectively identifying and attacking adversarial C2 nodes throughout execution. The only real issue identified was the tendency to attack these nodes as identified, rather than synchronizing the attack with the tempo of the operation.<sup>68</sup> This tendency could allow for reconstitution of the node in time to effect future operations. Simply destroying a node is not the goal in an effective C2W effort. The key is to

synchronize the destruction or degradation within the operational plan, producing the desired effects at the desired time.

### Summary

Despite the impressive successes of the coalition's application of the elements of C2W during Desert Storm, US Army forces at the division and corps level still suffer severe difficulties applying these same elements. Planning and integrating the synergistic application of C2W remains a problem for these units. One would think that the effects produced during Desert Storm would drive a an aggressive effort within the US Army to produce similar effects at a lower level. Though from the review of the CALL BCTP database, this does not appear to be the case.

## **CHAPTER 6 APPLICATION OF CRITERIA/CONCLUSION**

As stated in the introduction of the monograph, the battle dynamics of Force XXI provide the criteria for assessing the establishment of C2W as a BOS for Force XXI operations. Evaluating the contributions of C2W to each battle dynamic will provide insight into the value of its establishment as a BOS.

The centerpiece of battle command in Force XXI operations will be the digitized ABCS. The common situational awareness produced through ABCS will drive the Force XXI commander's decision making process. It will allow him to make decisions at a much faster pace. Critical to the effective use of the ABCS will be spectrum supremacy. The C2 Protect and C2 Attack functions of C2W stand ready to address this requirement. C2 Protect operations will identify an adversary's likely C2 Attack COAs, and develop

protection actions to defeat or minimize their effectiveness. Additionally C2 Attack operations will target the adversary's C2 systems, denying or degrading his use of the spectrum. Effective planning and execution of the two functions of C2W will go far in providing the spectrum dominance required in Force XXI.

Closely linked with battle command is the dynamic of battlespace. The key to this dynamic is for the commander to dominate his extended battlespace through an increased tempo. The tool to achieve this increased tempo is information. Information flow must be tailored to support the commander's needs and must be continuous and near instantaneous. Information systems development will provide for this tailoring and dissemination. C2W provides the necessary protection for these systems while at the same time attacking those of an adversary. Successful battlespace dominance in Force XXI operations will greatly depend on creating an information advantage, and as a result C2W will be a critical function in this dynamic.

The contributions of C2W in the dynamic of depth and simultaneous attack are also impressive. Clearly, protecting the flow of targeting data enabling the attacks is critical, but the systems approach to paralyzing an adversary through C2W is of even greater importance. By understanding the method in which an adversary controls his battlefield systems and attacking them in a coordinated and integrated manner, C2W is capable of producing information paralysis. Paralysis will greatly enhance the effect of depth and simultaneous attack, and at the same time reduce friendly losses by causing an adversary to fight in an autonomous instead of integrated manner.

C2W operations will also contribute significantly to the Force XXI dynamic of early entry. As friendly forces flow into the area of operations, C2W will be very effective in disrupting an adversary's ability to respond to these force deployments. A force in the process of deployment is extremely vulnerable. C2W can be very effective in protecting the force in the deployment stage. Additionally, C2W can protect the numerous information tethers necessary to support this early entry force. These information tethers will be critical to the effective control and application of early entry forces. C2W will play a critical role in effective early entry operations described in the Force XXI operational concept.

To maintain the increased tempo of operations described within Force XXI, CSS elements will require close connectivity with the supported commander. Similar to the dynamics of battle command and battlespace, effective C2W operations will be a critical enabler for this connectivity. By protecting the friendly flow of information, C2W will allow the CSS leader to quickly realize changes in the operational situation, requirements, and priorities. As a result, the CSS leader will be able to redirect the resources necessary to maintain the operational tempo required in the Force XXI operational environment.

C2W will be a critical function necessary to address the future conditions described in the five battle dynamics of Force XXI operations. As a result, based on the current definition of BOS, it warrants intense consideration as a BOS for Force XXI. From the study of CALL BCTP database, the principle problems found in planning and executing C2W operations currently center on ineffective integration and synchronization

of its elements. Identifying it as its own BOS will make great strides in addressing these inadequacies.

Under the US Army's current list of BOS, the elements of C2W are dispersed and in effect buried under different BOS. The elements of PSYOP, EW, and physical destruction fall under the Fires BOS.<sup>69</sup> One finds the elements of deception and OPSEC subordinate to the Mobility and survivability BOS.<sup>70</sup> Clearly this degrades their synergistic application. Bringing the elements under one critical function within the US Army is critical to producing the synergistic effects witnessed during Desert Storm. As long as the elements of this critical function remain subordinate to various other Army warfighting functions, C2W will remain ineffective and the operational concept for Force XXI will be greatly threatened.

The steam engine was a critical development in the evolution of the Industrial Age. However, its invention was not as important as the development of the capability to control the output of the engine. Controlling the output allowed inventors to tailor the power to their needs. Establishing control of the output through the use of a governor, set the conditions necessary for the exploitation of the steam engine in the Industrial Age.

With the development of information systems technology today and in the future, the possibility exists for C2W to take its place in importance in military operations in much the manner the governor did in the exploitation of steam. As military forces become further dispersed, as a result of increases in weapons lethality, a greater demand is placed on information flow. A commander will no longer be able to rely on person to person communication, this link will be replaced by information flowing from advanced

information systems. The protection of one's own information flow, and the attack of an adversary's, will likely prove to be the critical development within military operations in the Information Age.

Information is critical for a military organization to adapt to its operational environment. It is the basis for decision making. Without information feedback, the organization is unable to appropriately adapt to its environment, and as a result likely faces defeat. C2W provides the tool necessary to deny or degrade an adversary's feedback, at the same time providing for the protection of that of a friendly force.

Developing methods for the establishment and tailoring of information flow will clearly be a critical function for the U.S. Army in Force XXI. However, an equally important function for this force will be protecting this flow of information while attacking that of an adversary.

## Endnotes

- <sup>1</sup> TRADOC Pamphlet 525-5, Force XXI Operations, Fort Monroe, VA: Headquarters Training and Doctrine Command (TRADOC), 3-3.
- <sup>2</sup> FM 100-5, Glossary-1
- <sup>3</sup> Ibid.
- <sup>4</sup> Peter Senge, The Fifth Discipline (New York: Currency Doubleday, 1994), 6-7.
- <sup>5</sup> Chairman, Joint Chiefs of Staff, Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare (C2W) (Washington, DC: U.S. Government Printing Office, February 1996) 1-4.
- <sup>6</sup> Ibid., v.
- <sup>7</sup> Ibid., GL-8.
- <sup>8</sup> Chairman, Joint Chiefs of Staff, MOP 30, Command and Control Warfare (Washington, DC: U.S. Government Printing Office, 1993), 4.
- <sup>9</sup> Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, GL-11.
- <sup>10</sup> Headquarters, Department of the Army, FM 100-6, Information Operations (Washington, DC: U.S. Government Printing Office, 1996), 3-3.
- <sup>11</sup> FM 100-5, Operations, 6-9.
- <sup>12</sup> Jervis, Robert, "Hypothesis on Misperception," World Politics (Apr 68), 455.
- <sup>13</sup> Headquarters, Department of the Army, FM 90-2, Battlefield Deception (Washington, DC: U.S. Government Printing Office, 1988), 38-39.
- <sup>14</sup> JCS Pub 3-13.1, Joint Doctrine for Command and Control Warfare, GL-7.
- <sup>15</sup> Headquarters, Department of the Army, FM 34-1, Intelligence and Electronic Warfare Operations, (Washington, DC: U.S. Government Printing Office, 1994), 2-22.
- <sup>16</sup> Ibid., 2-21.
- <sup>17</sup> FM 100-6, Information Operations, 3-5.
- <sup>18</sup> Ibid., 3-6.
- <sup>19</sup> Ibid.
- <sup>20</sup> Ibid.
- <sup>21</sup> Ibid.
- <sup>22</sup> Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, II-4,5.
- <sup>23</sup> FM 100-6, Information Operations, 3-6.
- <sup>24</sup> Ibid.
- <sup>25</sup> Ibid., 3-9.
- <sup>26</sup> Ibid.
- <sup>27</sup> TRADOC Pam 525-5, Force XXI Operations, 3-3.
- <sup>28</sup> FM 100-5, Operations, Glossary-1
- <sup>29</sup> TRADOC Pam 525-5, Force XXI Operations, 3-4.
- <sup>30</sup> Ibid., 3-8.
- <sup>31</sup> Gen Gordon R. Sullivan, "A New Force for a New Century," Army, May 1994, 26.
- <sup>32</sup> Cpt Arthur S. DeGroat, "Information and Combat Power on the Force XXI Battlefield," Military Review, Nov-Dec 1995, p.56.
- <sup>33</sup> TRADOC Pam 525-5, Force XXI Operations, 3-10.



- <sup>34</sup> Ibid.
- <sup>35</sup> Gen Gordon R. Sullivan, "Moving into the 21st Century: America's Army and Modernization," Military Review, July 1993, 9.
- <sup>36</sup> Headquarters Training and Doctrine Command, Force XXI Division Organizational and Operational Concept (Draft) (Fort Monroe, VA: Hqs TRADOC, 1996), 14.
- <sup>37</sup> TRADOC Pam 525-5, Force XXI Operations, p. 3-13.
- <sup>38</sup> Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress (Washington DC: U.S. Government Printing Office, 1992) 77-78.
- <sup>39</sup> Ibid., 77.
- <sup>40</sup> Ibid., 77.
- <sup>41</sup> Ibid., 248.
- <sup>42</sup> Ibid., 249.
- <sup>43</sup> Ibid., 77.
- <sup>44</sup> Ibid., 536.
- <sup>45</sup> Ibid., 537.
- <sup>46</sup> Ibid., 537.
- <sup>47</sup> Ibid., 538.
- <sup>48</sup> Ibid., 538.
- <sup>49</sup> Ibid., 538.
- <sup>50</sup> Ibid., 150.
- <sup>51</sup> Ibid., 151.
- <sup>52</sup> Headquarters, Department of the Army, FM 101-5-1, Operational Terms and Graphics (Final Draft) (Washington, DC: US Government Printing Office, July 1995), 1-111.
- <sup>53</sup> Center for Army Lessons Learned (CALL) Battle Command Training Program (BCTP) Database, (Fort Leavenworth, KS) FY 94 BCTP Perceptions, 2 and FY 95 BCTP Perceptions, 14.
- <sup>54</sup> CALL BCTP Database, BCTP WFX Final Exercise Review (FER) 93-08, 86; 94-01, 91; 94-06, 214; 95-05, 136; 96-07, III-7-6; and FY 94 BCTP Perceptions, 2.
- <sup>55</sup> BCTP WFX FER 94-06, 130.
- <sup>56</sup> BCTP WFX FER 89-08, 55.
- <sup>57</sup> BCTP WFX FER 94-07, 273.
- <sup>58</sup> Ibid.
- <sup>59</sup> BCTP Perceptions FY 94, 13; BCTP Perceptions FY 95, 14.
- <sup>60</sup> BCTP WFX FER 92-03, 63; 93-08, 86; 94-01, 91; 94-06, 130; and BCTP Perceptions FY 94, 14.
- <sup>61</sup> BCTP Perceptions FY 94, 42; BCTP Perceptions FY 95, 45.
- <sup>62</sup> BCTP WFX FER 94-01, 57.
- <sup>63</sup> BCTP WFX FER 94-06, 130.
- <sup>64</sup> BCTP WFX FER 94-01, 57; BCTP WFX FER 94-06, 130.
- <sup>65</sup> BCTP WFX FER 96-07, III-7-6.
- <sup>66</sup> Ibid, III-7-13.
- <sup>67</sup> BCTP WFX FER FY 94/95 slides
- <sup>68</sup> BCTP Perceptions FY 94, 4-5; BCTP WFX FER 89-08, 55-56.

<sup>69</sup> Army Training and Doctrine Command, TRADOC PAM 11-9, Blueprint of the Battlefield (Fort Monroe, VA, 10 Sep 1993), 7-9.

<sup>70</sup> Ibid., 7-6.

## BIBLIOGRAPHY

### Books

- Alberts, David S. The Unlimited Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative. National Defense University, Washington, DC: U.S. Government Printing Office, 1991.
- Beniger, James R. The Control Revolution. Cambridge, Massachusetts: Harvard University Press, 1986.
- Brown, Anthony Cave. Bodyguard of Lies. New York: Harper Collins Publishers Inc., 1975.
- Campen, Alan D., ed. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA: AFCEA International Press, 1992.
- Kelly, Kevin. Out of Control. Reading, Massachusetts: Addison-Wesley Publishing Company, 1994.
- Senge, Peter M. The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Doubleday, 1990.
- Sun Tzu. The Art of War. translated by Samuel B. Griffith. London: Oxford University Press, 1963.
- Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown and Company, 1993.
- Waldrup, M. Michael. Complexity. New York: Simon and Schuster, 1992.

### Monographs, Theses, And Dissertations

- Boslego, David V. "The Relationship of Information To The Relative Combat Power Model In Force XXI Engagements." School of Advanced Military Studies Monograph, U.S. Command and General Staff College, Fort Leavenworth, Kansas, December 1995.

- Grymes, Robert D. "Command and Control Warfare in Forced Entry Operations." School of Advanced Military Studies Monograph, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, May 1995.
- Guthrie, Samuel A. "Knowledge-Based Operations: The "So What" of Information Warfare." School of Advanced Military Studies Monograph, U.S. Command and General Staff College, Fort Leavenworth, Kansas, May 1995.
- Hutcherson, Norman B. "Command and Control Warfare: Putting Another Tool in the Warfighter's Data Base." Air University, Maxwell Air Force Base, September 1994.
- Locke, Jeffrey S. "Command and Control Warfare: Promise and Challenge for the Operational Commander." Naval War College, Newport, Rhode Island, November
- Plucker, Ron C. "Command and Control Warfare-A New Concept For The Joint Operational Commander." Naval War College, Newport, Rhode Island, June 1993.
- Sexton, Joanne. "A Combatant Commander's Organizational View of Information Warfare and Command and Control Warfare." Naval War College, Newport, Rhode Island, June 1995.
- Tempestilli, Mark. "Waging Information Warfare: Making the Connection Between Information and Power In A Transformed World." U.S. Naval War College, Newport, Rhode Island, November 1995.
- Watson, David D. "Information Warfare and the Operational Art." Naval War College, Newport, Rhode Island, February 1996.

#### Magazines And Periodicals

- Blount, Kerry A. "Wrestling with Information Warfare's 'Dark Side'." Army, February 1996, 9-15.
- Blount, Kerry A. and Lauren D. Kohn. "C2 Warfare in FM 100-6." Military Review, July-August 1995, 66-69.
- Boyd, Morris J. "A Milestone in the Army's Journey into the Next Century." Army, May 1995, 25-30.

- Campan, Alan D. "Assessments Necessary in Coming To Terms with Information Warfare." Signal, June 1996, 47-50.
- DeGroat, Arthur S and David C. Nilsen. "Information and Combat Power on the Force XXI Battlefield." Military Review, November-December 1995, 56-62.
- DiNardo, R.L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." Airpower Journal, Winter 1995, 69-79
- Fitzgerald, Mary C. "Russian Views on Information Warfare." Army, May 1994, 57-60.
- Hartzog, William W. "Crossing the Threshold into a New Age." Army, May 1995, 21-24.
- Hill, Martin R. "It is Time to Get on with Information Warfare." Defense Intelligence Journal, Spring 1996, 25-41.
- Jablonsky, David. "US Military Doctrine and The Revolution in Military Affairs." Parameters, Autumn 1994, 19-36.
- Jensen, Owen E. "Information Warfare Principles of Third-Wave War." Airpower Journal, Winter 1994, 35-43.
- Madigan, James C. and George E. Dodge. "Battle Command: A Force XXI Imperative." Military Review, November 1994, 29-39.
- Mahnken, Thomas G. "War in the Information Age." Joint Forces Quarterly, Winter 1995-96, 39-43.
- Maynard, Wayne K. "The New American Way of War." Military Review, November 1993, 5-17.
- Mann, Edward. "Desert Storm: The First Information War." Airpower Journal, Winter 1994, 4-13.
- Miller, John E. and Kurt C. Reitingen. "Force XXI Battle Command." Military Review, July-August 1995, 5-9.
- Morris, J. Boyd and Michael Woodgred. "Force XXI Operations." Military Review, November 1994, 17-28.
- Ohle, David H. "The Campaign Plan." Army, February 1995, 18-23.

- Owens, William A. "The Emerging System of Systems." Proceedings, May 1995, 35-39.
- Reimer, Dennis J. "Reengineering Forces Command for the 21st Century." Army, May 1995, 31-35.
- Riccardelli, Richard F. "The Information and Intelligence Revolution." Military Review, September-October 1995, 82-87.
- Rigby, Joe W. "Digitizing Force XXI: A Team Effort." Army, May 1995, 36-45.
- Robinson, Clarence A., Jr. "Army Information Operations Protect Command and Control." Signal, July 1996, 47-50.
- Robinson, Clarence A., Jr. "Rapid Technology Growth Spawns Land Information Warfare Activity." Signal, July 1996, 51-56.
- Rona, Thomas P. "Information Warfare: An Age Old Concept With New Insights." Defense Intelligence Journal, Spring 1996, 53-69.
- Ross, Jimmy D. "Winning the Information War." Army, February 1994, 27-32.
- Ryan, Donald E., Jr. "Implications of Information-Based Warfare." Joint Forces Quarterly, Autumn/Winter 1994-95, 114-116.
- Ryan, Julie, John Woloschek and Barry Leven. "Complexities In Conducting Information Warfare." Defense Intelligence Journal, Spring 1996, 69-82.
- Stanley, Verle R. and Phillip L. Noggle. "Command & Control Warfare- Seizing the Initiative." Signal, April 1984, 23-28.
- Stevens, Halbert F. "Information Dominance: The New High Ground." Defense Intelligence Journal, Spring 1996, 43-52.
- Struble, Dan. "What is Command and Control Warfare?" Naval War College Review, Summer 1995, 89-98.
- Sullivan, Gordon R. "Moving into the 21st Century: America's Army and Modernization." Military Review, July 1993, 2-11.
- Sullivan, Gordon R. and James M. Dubik. "Land Warfare in the 21st Century." Military Review, September 1993, 13-32.

Sullivan, Gordon R. "A New Force for a New Century." Army, May 1994, 24-27.

Sullivan, Gordon R. and James M. Dubik. "War in the Information Age." Military Review, April 1994, 46-62.

Vincent, Gary A. "In the Loop, Superiority in Command and Control." Airpower Journal, Summer 1992, 15-25.

Vincent, Gary A. "A New Approach to Command and Control, The Cybernetic Design." Airpower Journal, Summer 1993, 24-38.

Military Manuals, Publications, And Government Documents

Center for Army Lessons Learned. BCTP Database. Fort Leavenworth, KS, FY 1989-1996.

Chairman, Joint Chiefs of Staff. Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare. Washington, D.C.: Office of the Joint Chiefs of Staff, February 1996.

\_\_\_\_\_. Memorandum of Policy No. 30, Command and Control Warfare. Washington, D.C.: Office of the Joint Chiefs of Staff, March 1993.

Department of Defense. Conduct of the Persian Gulf War: Final Report to Congress. Washington, D.C.: Office of the Secretary of Defense, 1992.

United States Army. FM 33-1, Psychological Operations. Washington, D.C.: Department of the Army, 1993.

\_\_\_\_\_. FM 34-1, Intelligence and Electronic Warfare Operations. Washington D.C., Department of the Army, 1994.

\_\_\_\_\_. FM90-2, Battlefield Deception. Washington, D.C., Department of the Army, 1988.

\_\_\_\_\_. FM 100-5, Operations. Washington, D.C., Department of the Army, 1993.

\_\_\_\_\_. FM 100-6, Information Operations. Washington, D.C., Department of the Army, 1996.

- TRADOC Pam 525-5, Force XXI Operations. Fort Monroe, VA: U.S. Army Training and Doctrine Command, 1 August 1994.
- TRADOC Pam 525-69, Concept for Information Operations. Fort Monroe, VA: U.S. Army Training and Doctrine Command, August 1995.
- TRADOC Pam 525-200-1, Battle Command. Fort Monroe, VA: U.S. Army Training and Doctrine Command, December 1994.
- Force XXI Division Organizational and Operational Concept (Draft). Fort Monroe, VA: U.S. Army Training and Doctrine Command, 1996.